ふじみ野市情報セキュリティポリシー

第６版

平成１８年	９月	６日	策　　定
平成２４年	３月２３日		一部改正
平成２６年	１月２７日		全部改正
平成２８年	９月	１日	全部改正
令和　２年	２月１８日		全部改正
令和　４年	３月	３日	全部改正
令和　５年	４月	１日	全部改正

目次

ふじみ野市情報セキュリティ基本方針

ふじみ野市情報セキュリティ対策基準

序　情報セキュリティポリシーの構成

ふじみ野市情報セキュリティポリシーとは、本市が保有する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的にとりまとめたものであり、情報セキュリティ対策の頂点に位置する。情報セキュリティポリシーは、情報資産に関する業務に携わる全職員及び委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。

しかし一方では、情報の処理技術や通信技術等の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

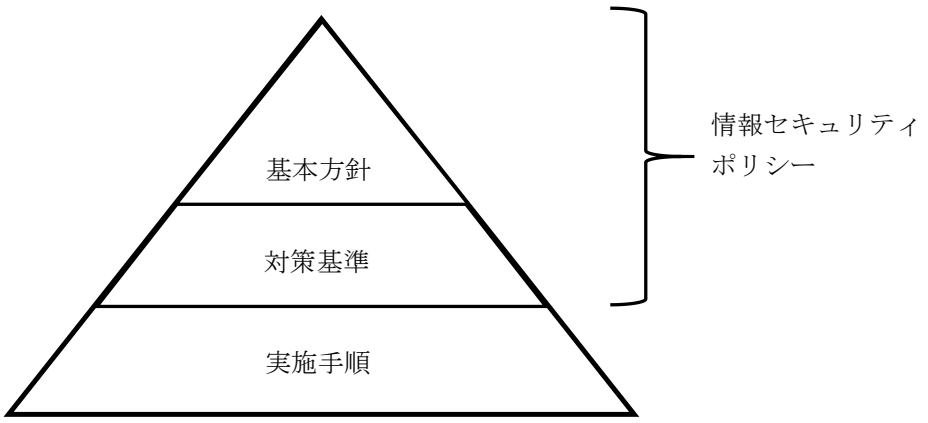
このようなことから、情報セキュリティポリシーは一定の普遍性を備えた「情報セキュリティ基本方針」と、情報資産を取り巻く状況変化にも適切に対応する「情報セキュリティ対策基準」の２階層で構成する。

また、本情報セキュリティポリシーに基づき、具体的な情報セキュリティ対策の運用マニュアルとして、「情報セキュリティ実施手順」を策定し、総合的な情報セキュリティ対策を実施する。

情報セキュリティポリシーの構成

文　書　名		内　　容
ふじみ野市情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する基本的な考え方
	情報セキュリティ対策基準	情報セキュリティ基本方針に基づき、共通の情報セキュリティ対策の基準を定める
情報セキュリティ実施手順		対策基準に基づき、具体的なシステムの手順手続きに対し、個別の実施事項を定める

情報セキュリティポリシーに関する体系図



ふじみ野市情報セキュリティ基本方針

1　目的

この基本方針は、市が保有する情報資産の機密性、完全性及び可用性を維持するため、市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2　定義

(1) ネットワーク

コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。

(2) 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(3) 情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

(4) 情報セキュリティポリシー

この基本方針及び情報セキュリティ対策基準をいう。

(5) 機密性

情報にアクセスすることを認められた者だけが、その情報にアクセスできる状態を確保することをいう。

(6) 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(7) 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、その情報にアクセスできる状態を確保することをいう。

(8) マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

(9) LGWAN接続系

LGWANに接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。

(10) インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(11) 通信経路の分割

LGWAN接続とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(12) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

3　対象とする脅威

市は、情報資産に対する脅威として、次に掲げる脅威を想定し、情報セキュリティ対策を実施する。

(1) 不正アクセス、コンピュータウイルス攻撃、サービス不能攻撃等のサイバー攻撃及び部外者の侵入等の意図的な要因による情報資産の漏えい、破壊、改ざん、消去、重要情報の詐取、内部不正等

(2)情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい、破壊、消去等

(3) 地震、落雷、火災等の災害によるサービス及び業務の停止等

(4) 大規模及び広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

(5) 電力供給、水道供給、通信の途絶等のインフラの障害からの波及等

4　適用範囲

(1) 行政機関の範囲

この基本方針が適用される行政機関は、市長、地方公営企業、議会事務局及び各行政委員会（小中学校を除く。）とする。

(2) 情報資産の範囲

この基本方針が対象とする情報資産は、次に掲げるとおりとする。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

ウ　情報システムの仕様書及びネットワーク図等のシステム関連文書

5　職員等の遵守義務

職員、非常勤職員及び臨時職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

6　情報セキュリティ対策

市は、上記３の脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講じる。

(1) 組織体制

市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

(2) 情報資産の分類と管理

市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類により情報セキュリティ対策を実施する。

(3) 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

ア　マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

イ　LGWAN接続系においては、LGWANと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

ウ　インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(4) 物理的セキュリティ

サーバ、情報システム室、通信回線、職員等の使用するパソコン等の管理について物理的な対策を講じる。

(5) 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行うなどの人的な対策を講じる。

(6) 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(7) 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等について情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

(8) 業務委託と外部サービスの利用

業務委託を行う場合には、委託業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

(9) 評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

7　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果において、情報セキュリティポリシーの見直しが必要となった場合又は情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

9　情報セキュリティ対策基準の策定

市は、上記６から８までに規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

１０　情報セキュリティ実施手順の策定

市は、情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

ふじみ野市情報セキュリティ対策基準

1　趣旨

この対策基準は、ふじみ野市情報セキュリティ基本方針に規定する対策等の実施について必要な事項を定めたものである。

2　組織体制

(1) 最高情報セキュリティ責任者（Chief Information Security Officer。以下「CISO」という。）

ア　CISOは、副市長とする。CISOは、市における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

イ　CISOは、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めることができる。

ウ　CISOは、情報セキュリティインシデントに対処するための体制（CSIRT:Computer Security Incident Response Team。以下「CSIRT」という。）を整備し、役割を明確化する。

エ　CISOは、CISOを助けて本市における情報セキュリティに関する事務を整理し、CISOの命を受けて本市の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者（以下「副CISO」という。）１人を必要に応じて置くことができる。

オ　CISOは、本対策基準に定められた自らの担務を、副CISOその他の本対策基準に定める責任者に担わせることができる。

(2) 統括情報セキュリティ責任者

ア　CISO直属の統括情報セキュリティ責任者は、総合政策部長とする。

イ　統括情報セキュリティ責任者は、情報資産の管理及び情報セキュリティ対策に関しCISO及び副CISOを補佐するとともに、次の権限及び責任を有する。

(ｱ) 市の全てのネットワークにおける開発、設定の変更、運用、見直し等を行うこと。

(ｲ) 市の全てのネットワークにおける情報セキュリティ対策に関すること。

(ｳ) 情報セキュリティ責任者及び情報セキュリティ管理者に対して、情報セキュリティに関する指導及び助言を行うこと。

(ｴ) 市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISOの指示に従い、CISOが不在の場合には自らの判断により必要かつ十分な措置を行うこと。

(ｵ) 市の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持及び管理を行うこと。

ウ　統括情報セキュリティ責任者は､緊急時等の円滑な情報共有を図るため、CISO、統括情報セキュリティ責任者、情報セキュリティ責任者及び情報セキュリティ管理者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

エ　統括情報セキュリティ責任者は、緊急時には CISO に早急に報告を行うとともに、回復のための対策を講じなければならない。

オ　統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じてCISOにその内容を報告しなければならない。

カ　統括情報セキュリティ責任者は、必要があると認めるときは、その権限に属する事務を情報管理部門の課の長に処理させることができる。

(3) 情報セキュリティ責任者

ア　情報セキュリティ責任者は、各部局の長、地方公営企業部局の長、議会事務局の長及び各行政委員会事務局（小中学校を除く。）の長とする。

イ　情報セキュリティ責任者は、次に掲げる権限及び責任を有する。

(ｱ) その所管する部局等の統括的な情報セキュリティ対策に関すること。

(ｲ) その所管する部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的なこと。

(ｳ) その所管する部局等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに職員等に対する教育、訓練、助言及び指示を行うこと。

(4) 情報セキュリティ管理者

ア　情報セキュリティ管理者は、各部局、地方公営企業、議会事務局及び各行政委員会事務局（小中学校を除く。）の課長相当職（各部局の出先機関においては、当該出先機関の長）とする。

イ　情報セキュリティ管理者は、次の権限及び責任を有する。

(ｱ) その所管する課等の情報セキュリティ対策に関すること。

(ｲ) その所管する課等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合は、CISO、統括情報セキュリティ責任者及び情報セキュリティ責任者に速やかに報告を行い、指示を仰ぐこと。

(ｳ) 所管する情報システムにおける開発、設定の変更、運用、見直し等に関すること。

(ｴ) 所管する情報システムにおける情報セキュリティに関すること。

(ｵ) 所管する情報システムに係る情報セキュリティ実施手順の維持及び管

理を行うこと。

(5) 情報セキュリティ担当者

ア　情報セキュリティ担当者は、情報化推進リーダーをもって充てる。情報化推進リーダーは、情報セキュリティ管理者がその所属職員の中から指名した者とする。

イ　情報セキュリティ担当者は、情報セキュリティ管理者の指示等に従い、その所属する課室及び施設等の情報セキュリティ対策等の向上を図るものとする。

(6) デジタルトランスフォーメーション（ＤＸ）推進会議（以下「ＤＸ推進会議」という。）

市の情報セキュリティ対策を統一的に行うため、ＤＸ推進会議において、情報セキュリティポリシー等の情報セキュリティに関する重要な審議を行う。

(7) 兼務の禁止

ア　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

イ　情報セキュリティ監査の実施において、やむを得ない場合を除き、情報セキュリティ対策の監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

(8) CSIRT の設置・役割

ア　CISO は、CSIRT を整備し、その役割を明確化しなければならない。

イ　CISO は、CSIRT に所属する職員等を選任し、その中から CSIRT 責任者を置かなければならない。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定めなければならない。

ウ　CISO は、情報セキュリティインシデント（情報セキュリティに関する障害、事故及びシステム上の欠陥のことをいう。以下同じ。）の統一的な窓口の機能を有する組織（Point of Contact。以下「PoC」という。）を置くものとし、情報セキュリティインシデントについて部局等から報告を受けた場合は、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

エ　PoC は、CISO による情報セキュリティ戦略の意思決定が行われた際は、その内容を関係部局等に提供しなければならない。

オ　PoC は、情報セキュリティインシデントを認知した場合は、CISO、総務省、埼玉県へ報告しなければならない。

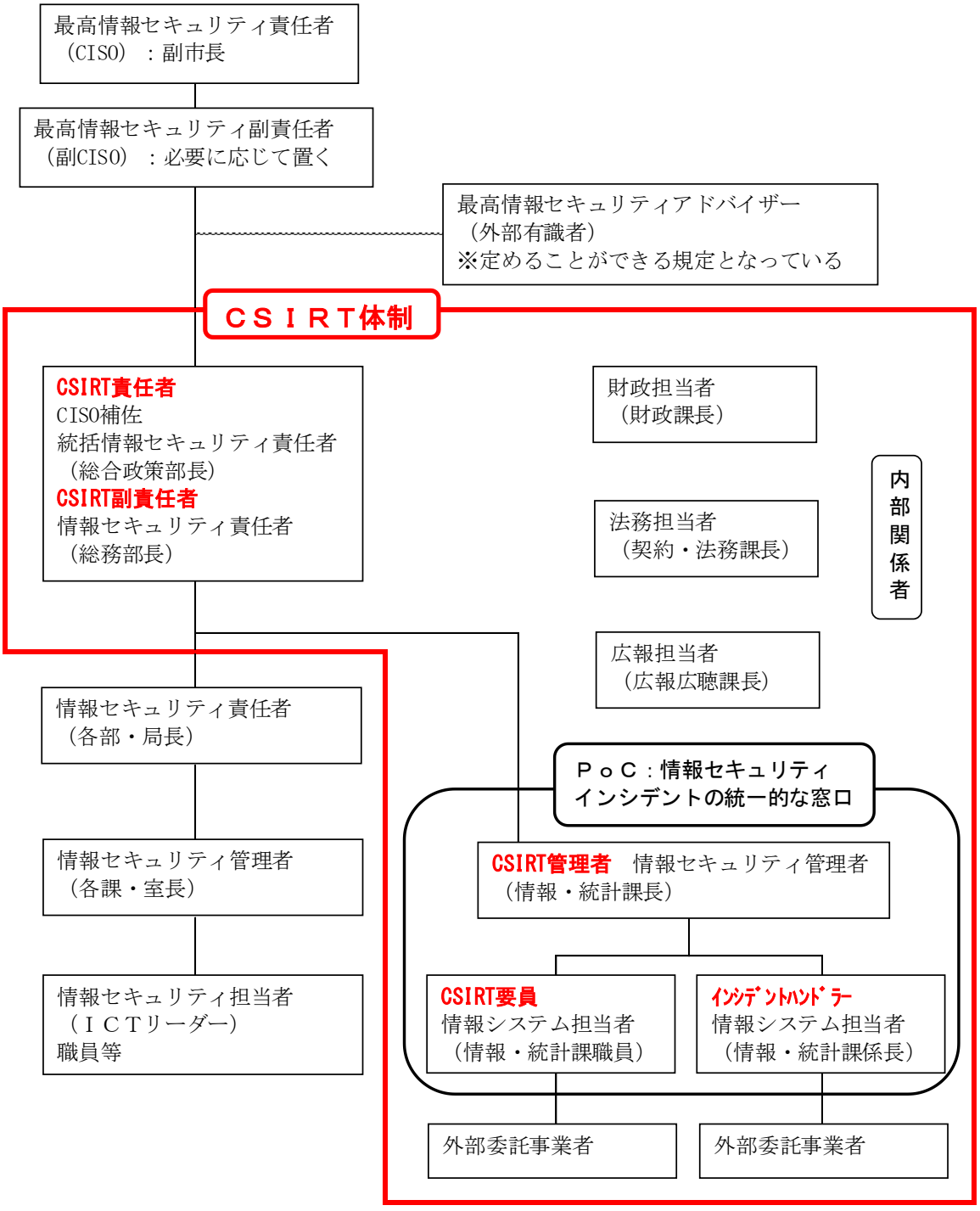
カ　PoC は、情報セキュリティインシデントを認知した場合は、その重要度、影響範囲等を勘案し、報道機関への通知又は公表対応を行わなければならない。

キ　PoC は、情報セキュリティに関して、関係機関や他の地方公共団体の情

報セキュリティに関する統一的な窓口の機能を有する部署、委託事業者等との情報共有を行わなければならない。

ク　CISO は、PoC を設置したときは、PoC への連絡手段を公表しなければならない。

※組織体制図


最高情報セキュリティ責任者
（CISO）：副市長
最高情報セキュリティ副責任者
（副CISO）：必要に応じて置く
最高情報セキュリティアドバイザー
（外部有識者）
※定めることができる規定となっている
ＣＳＩＲＴ体制
CSIRT責任者
CISO補佐
統括情報セキュリティ責任者
（総合政策部長）
CSIRT副責任者
情報セキュリティ責任者
（総務部長）
財政担当者
（財政課長）
法務担当者
（契約・法務課長）
広報担当者
（広報広聴課長）
内部関係者
情報セキュリティ責任者
（各部・局長）
情報セキュリティ管理者
（各課・室長）
情報セキュリティ担当者
（ＩＣＴリーダー）
職員等
ＰｏＣ：情報セキュリティインシデントの統一的な窓口
CSIRT管理者　情報セキュリティ管理者
（情報・統計課長）
CSIRT要員
情報システム担当者
（情報・統計課職員）
ｲﾝｼﾃﾞﾝﾄﾊﾝﾄﾞﾗｰ
情報システム担当者
（情報・統計課係長）
外部委託事業者
外部委託事業者

3　情報資産の分類と管理

(1) 情報資産の分類

市における情報資産は、機密性、完全性及び可用性に基づき、次のとおり分類し、必要に応じ取扱制限を行うものとする。

機密性による情報資産の分類

分類	分類基準	取扱制限
機密性３	行政事務で取り扱う情報資産のうち秘密文書に相当する機密性を要する情報資産	・支給以外の端末での作業の原則禁止（機密性３の情報資産に限る） ・必要以上の複製及び配付の禁止 ・保管場所の制限及び保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信又は情報資産の運搬若しくは提供時における暗号化・パスワード設定及び鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理基準の作成 ・電磁的記録媒体の施錠可能な場所への保管
機密性２	行政事務で取り扱う情報資産のうち秘密文書に相当する機密性ではないが、直ちに一般に公表することを前提としていない情報資産	
機密性１	機密性２又は機密性３の情報資産以外の情報資産	―

完全性による情報資産の分類

分類	分類基準	取扱制限
完全性２	行政事務で取り扱う情報資産のうち改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ及び電子署名付与 ・外部で情報処理を行う際の安全管理基準の作成 ・電磁的記録媒体の施錠可能な場所への保管
完全性１	完全性２の情報資産以外の情報資産	―

可用性による情報資産の分類

分類	分類基準	取扱制限
可用性２	行政事務で取り扱う情報資産のうち滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ及び指定する時間内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性１	可用性２の情報資産以外の情報資産	―

(2) 情報資産の管理

ア　管理責任

(ｱ) 情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

(ｲ) 情報資産が複製又は伝送された場合においても、(1)の分類に基づき管理しなければならない。

イ　情報資産の分類の表示

職員等は、情報資産についてファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー及びフッター等）、格納する電磁的記録媒体のラベル、文書の隅等に情報資産の分類を表示し、必要に応じて取扱制限を明示する等の適切な管理を行わなければならない。

ウ　情報の作成

(ｱ) 職員等は、業務上必要のない情報を作成してはならない。

(ｲ) 情報を作成する者は、情報の作成時に(1)の分類により当該情報の分類及び取扱制限を定めなければならない。

(ｳ) 情報を作成する者は、作成途中のいかんにかかわらず情報の紛失、流出等を防止しなければならない。また、情報の作成途中で不要になった場合は、当該情報を消去しなければならない。

エ　情報資産の入手

(ｱ) 職員等が作成した情報資産を入手した者は、入手元の情報資産の分類による取扱いをしなければならない。

(ｲ) 委託業者等の職員等以外の者が作成した情報資産を入手した者は、(1)の分類により当該情報の分類及び取扱制限を定めなければならない。

(ｳ) 情報資産を入手した者は、入手した情報資産の分類が不明な場合は、情報セキュリティ管理者に判断を仰がなければならない。

オ　情報資産の利用

(ｱ) 情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

(ｲ) 情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。

(ｳ) 情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合は、重要性分類の上位の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

カ　情報資産の保管

(ｱ) 情報セキュリティ管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

(ｲ) 情報セキュリティ管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

(ｳ) 情報セキュリティ管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を想定し、当該媒体が損害を受けないような措置を講じなければならない。

(ｴ) 情報セキュリティ管理者は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合は、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

キ　情報の送信

(ｱ) 電子メール等により機密性２以上の情報資産を送信する者は、情報セキュリティ管理者の許可を得なければならない。

(ｲ) 電子メール等により機密性２以上の情報を送信する者は、必要に応じてパスワード等による暗号化を行わなければならない。

ク　情報資産の運搬

(ｱ) 車両等により機密性２以上の情報資産を運搬する者は、必要に応じて鍵付きのケース等に格納し、パスワード等による暗号化を行うなど、情報資産の不正利用を防止するための措置を講じなければならない。

(ｲ) 機密性２以上の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

ケ　情報資産の提供及び公表

(ｱ) 機密性２以上の情報資産を外部に提供する者は、必要に応じてパスワード等による暗号化を行わなければならない。

(ｲ) 機密性２以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

(ｳ) 情報セキュリティ管理者は、住民に公開する情報資産について完全性を確保しなければならない。

コ　情報資産の廃棄等

(ｱ) 情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

(ｲ) 情報資産の廃棄やリース返却等を行う者は、行った処理について日時、担当者及び処理内容を記録しなければならない。

(ｳ) 情報資産の廃棄やリース返却等を行う者は、情報セキュリティ管理者の許可を得なければならない。

機密性に応じた情報資産の廃棄等の方法

分類	機器の廃棄等の方法	確実な履行を担保する方法
(1)マイナンバー利用事務系の領域において住民情報を保存する記憶媒体※マイナンバー利用事務系：社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ	当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすることが適当である。 なお、対象となる機器について、リース契約により調達する場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行う。この場合、予め仕様に明記のうえ、機器の廃棄方法を契約において明記することが望ましい。	職員が左記措置の完了まで立ち会いによる確認を行うほか、庁舎内において後述(3)で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の完了証明書により確認する。当該完了証明書については、破壊の証拠写真が添付されるとともに、その提出期限が定められていることが望ましい。
(2)機密性２以上に該当する情報を保存する記憶媒体（上記(1)に該当するものを除く。）	一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うことが適当である。 具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③OS等からのアクセスが不可	庁舎内において後述(3)で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。

	能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択することが適当である。	
(3)機密性１に該当する情報を保存する記憶媒体	一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去することが適当である。 具体的には、(2)に記述した方法①～⑤のほか、OS等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去する方法がある。 OS及び記憶装置の初期化（フォーマット等）による方法は、HDDの記憶演算子にはデータの記憶が残った状態となるため、適当ではない。	庁舎内において消去を実施し、職員が作業完了を確認する方法など適切な方法により確認を行う。
※上記(1)は、オンプレミスの場合を想定したもの（ハウジングやプライベートクラウドを含む）		

4　情報システム全体の強靭性の向上

(1) マイナンバー利用事務系

ア　マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(ＭＡＣアドレス、ＩＰアドレス)及びアプリケーションプロトコル(ポート番号)のレベルでの限定を行わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWAN を経由して、インターネ

ット等とマイナンバー利用事務系との双方向通信でのデータ移送を可能とする。

イ　情報アクセス及び持ち出しにおける対策

(ｱ) 情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証(多要素認証)を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。

(ｲ) 情報の持ち出し不可設定

原則として、ＵＳＢメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

(2) LGWAN 接続系

ア　LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

(ｱ) インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送するメールテキスト化方式

(ｲ) インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

(ｳ) 危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

(3) インターネット接続系

ア　インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

イ　都道府県及び市区町村のインターネットとの通信を集約する自治体情報セキュリティクラウドに参加するとともに、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

5　物理的セキュリティ

(1) サーバ等の管理

ア　機器の取付け

情報セキュリティ管理者は、サーバ等の機器の取付けを行う場合は、火災、水害、ほこり、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定するなど必要な措置を講じなければならない。

イ　サーバの冗長化

(ｱ) 情報セキュリティ管理者は､所管する重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを冗長化し、同一データを保持しなければならない。

(ｲ) 情報セキュリティ管理者は、所管するメインサーバに障害が発生した場合は、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。

ウ　機器の電源

(ｱ) 情報セキュリティ管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、所管するサーバ等の機器の電源について停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

(ｲ) 情報セキュリティ管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、所管するサーバ等の機器を保護するための措置を講じなければならない。

エ　通信ケーブル等の配線

(ｱ) 情報セキュリティ管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、所管する通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用するなど必要な措置を講じなければならない。

(ｲ) 情報セキュリティ管理者は、所管する主要な箇所の通信ケーブル及び電源ケーブルについて､施設管理部門から損傷等の報告があった場合は、施設管理部門と連携して対応しなければならない。

(ｳ) 情報セキュリティ管理者は、所管するネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置するなど適正に管理しなければならない。

(ｴ) 情報セキュリティ管理者は、自ら又は契約により操作を認められた委託事業者以外の者が配線の構造を変更及び追加できないように必要な措置を施さなければならない。

オ　機器の定期保守及び修理

(ｱ) 情報セキュリティ管理者は、所管する可用性２のサーバ等の機器の定期保守を実施しなければならない。

(ｲ) 情報セキュリティ管理者は、電磁的記録媒体を内蔵する機器を事業者に修理させる場合は、内容を消去した状態で行わせなければならない。ただし、内容を消去できない場合は、情報セキュリティ管理者は、事業者に故障を修理させるに当たり、修理を委託する事業者との間で、守秘義務契約を締結するなどして、秘密保持体制の確認等を行わなければならない。

カ　庁外への機器の設置

情報セキュリティ管理者は、所管するサーバ等の機器を庁外に設置する場合は、統括情報セキュリティ責任者の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

キ　機器の廃棄等

情報セキュリティ管理者は、機器を廃棄、リース返却等する場合は、機器内部の記憶装置から全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

(2) 管理区域（情報システム室等）の管理

ア　管理区域の構造等

(ｱ) 管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋（以下「情報システム室」という。）並びに電磁的記録媒体の保管庫をいう。

(ｲ) 情報セキュリティ管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、可能な限り管理区域を地階又は１階に設けてはならない。また、外部からの侵入が容易にできないようにしなければならない。

(ｳ) 情報セキュリティ管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアの数は、必要最小限とし、鍵、監視機能、警報装置等によって、許可されていない者の立入りを防止しなければならない。

(ｴ) 情報セキュリティ管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

(ｵ) 情報セキュリティ管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。

(ｶ) 情報セキュリティ管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器及び電磁的記録媒体等に影響を与えないようにしなければならない。

イ　管理区域の入退室管理等

(ｱ) 情報セキュリティ管理者は、管理区域への入退室について、許可された者のみに限定し、ＩＣカード又は指紋認証等の生体認証及び入退室管理簿の記載による入退室管理を行わなければならない。

(ｲ) 職員等及び委託事業者は、管理区域に入室する場合は、身分証明書等を携帯し、管理区域を所管する情報セキュリティ管理者から求めがあったときは、これを提示しなければならない。

(ｳ) 情報セキュリティ管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

(ｴ) 情報セキュリティ管理者は、機密性２以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しない、又は個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

ウ　機器等の搬入出

(ｱ) 情報セキュリティ管理者は、搬入する機器等が既存の情報システムに与える影響についてあらかじめ職員又は委託事業者に確認を行わせなければならない。

(ｲ) 情報システム室に機器等を搬入出する場合は、情報セキュリティ管理者は、情報システム室への入室を許可された職員を立ち会わせなければならない。

(3) 通信回線及び通信回線装置の管理

ア　統括情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。

イ　統括情報セキュリティ責任者は、 外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

ウ　統括情報セキュリティ責任者は、行政系のネットワークを総合行政ネットワーク（LGWAN）に集約するように努めなければならない。

エ　統括情報セキュリティ責任者は、機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合は、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ送受信される情報の暗号化を行うものとする。

オ　統括情報セキュリティ責任者は､ネットワークに使用する回線について、伝送途中に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

カ　統括情報セキュリティ責任者は、可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じて回線を冗長構成にする等の措置を講じるものとする。

(4) 職員等の利用する端末及び電磁的記録媒体等の管理

ア　情報セキュリティ管理者は、盗難防止のため、職員等が執務室等で使用するパソコンのワイヤーでの固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠保管等の物理的措置を講じなければならない。

イ　情報セキュリティ管理者は、電磁的記録媒体に記録した情報について保存する必要がなくなった場合は、当該情報を速やかに消去しなければならない。

ウ　情報セキュリティ管理者は、端末の起動時及び情報システムへのログイ

ン時にパスワード、ＩＣカード、或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。

エ　情報セキュリティ管理者は、マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証）を行うよう設定しなければならない。

オ　情報セキュリティ管理者は、パソコン又はモバイル端末にデータを暗号化する機能又はセキュリティチップが搭載されている場合は、これを有効に活用しなければならない。

カ　情報セキュリティ管理者は、電磁的記録媒体を使用する場合は、データを暗号化する機能が当該電磁的記憶媒体に備わっているものを使用しなければならない。

キ　情報セキュリティ管理者は、モバイル端末を庁外で使用する場合は、ウからオまでの対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。

6　人的セキュリティ

(1) 職員等の遵守事項

ア　職員等の遵守事項

(ｱ) 情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

(ｲ) 業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

(ｳ) モバイル端末、電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

a　CISO は、機密性２以上、可用性２又は完全性２のいずれかに該当する情報資産を外部で処理する場合は、別に安全管理措置に関する基準を定めなければならない。

b　職員等は、市のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合は、情報セキュリティ管理者の許可を得なければならない。

c　職員等は、外部で情報処理業務を行う場合は、情報セキュリティ管理者の許可を得なければならない。

(ｴ) 支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

a　職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に使用するために持ち込んではならない。ただし、支給以外の端末の業務利用の可否判断を CISO が行った後に、業務上必要な場合は、統括情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ責任者の許可を得て、これらを使用することができる。

b　職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を外部において業務に使用する場合は、情報セキュリティ責任者の許可を得なければならず、かつ、安全管理措置を遵守しなければならない。

(ｵ) 持ち出し及び持ち込みの記録

情報セキュリティ管理者は、パソコン、モバイル端末及び電磁的記録媒体の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

(ｶ) パソコン及びモバイル端末におけるセキュリティ設定変更の禁止

職員等は、パソコン及びモバイル端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

(ｷ) 机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用され、又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン及びモバイル端末のロック、電磁的記録媒体及び文書等の容易が閲覧されない場所への保管等の適正な措置を講じなければならない。

(ｸ) 退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合は、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

イ　非常勤及び臨時職員等への対応

(ｱ) 情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、非常勤及び臨時職員等に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び臨時職員等が守るべき内容を理解させ、また実施及び遵守させなければならない。

(ｲ) 情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、非常勤及び臨時職員等の採用の際に、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

(ｳ) インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤及び臨時職員等にパソコン又はモ

バイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

ウ　情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び情報セキュリティ実施手順を閲覧できるように、これらを掲示しなければならない。

エ　委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発、保守等を委託事業者に発注する場合は、再委託事業者も含めて、情報セキュリティポリシー等のうち委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

(2) 研修及び訓練

ア　情報セキュリティに関する研修及び訓練

CISOは、定期的に情報セキュリティに関する研修及び訓練を実施しなければならない。

イ　研修計画の策定及び実施

(ｱ) CISOは、幹部を含め全ての職員等に対する情報セキュリティに関する研修計画の策定及びその実施体制の構築を定期的に行うものとする。

(ｲ) 研修計画を策定する場合は、職員等は、毎年度１回以上の情報セキュリティ研修を受講できるようにしなければならない。

(ｳ) CISOは、新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

(ｴ) 研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報セキュリティ担当者及びその他の職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

(ｵ) 情報セキュリティ管理者は、所管する課室等の研修の実施状況を記録し､統括情報セキュリティ責任者及び情報セキュリティ責任者に対して、報告しなければならない。

(ｶ) 統括情報セキュリティ責任者は､研修の実施状況を分析､評価し､CISOに情報セキュリティ対策に関する研修の実施状況について報告しなければならない。

(ｷ) 職員等の情報セキュリティ研修の実施状況については、毎年度１回、ＤＸ推進会議に対して報告しなければならない。

ウ　緊急時対応訓練

(ｱ) CISOは、緊急時を想定した訓練を定期的に実施しなければならない。

(ｲ) 訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓

練実施の体制、範囲等を定めるものとし、効果的に実施できるようにしなければならない。

エ　研修及び訓練への参加

職員等は、ア及びウに規定する研修及び訓練に参加しなければならない。

(3) 情報セキュリティインシデント

ア　庁内での情報セキュリティインシデントの報告

(ｱ) 職員等は、情報セキュリティインシデントを認知した場合は、速やかに情報セキュリティ管理者及びPoCに報告しなければならない。

(ｲ) 報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者に報告しなければならない。

(ｳ) 情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、CISO及び情報セキュリティ責任者に報告するものとする。

イ　住民等外部からの情報セキュリティインシデントの報告

(ｱ) 職員等は、市が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合は、情報セキュリティ管理者に報告しなければならない。

(ｲ) (ｱ)の報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者に報告しなければならない。

(ｳ) 情報セキュリティ管理者は、情報セキュリティインシデントについて、必要に応じてCISO及び情報セキュリティ責任者に報告するものとする。

ウ　情報セキュリティインシデントにおける原因の究明、記録、再発防止等

(ｱ) CSIRTは、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

(ｲ) CSIRTは、情報セキュリティインシデントであると評価した場合、CISOに速やかに報告しなければならない。

(ｳ) CSIRTは、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。

(ｴ) CSIRTは、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデント原因究明の結果から、再発防止策を検討し、CISOに報告しなければならない。

(ｵ) CISOは、(ｲ)により報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

(4) ＩＤ及びパスワード等の管理

ア　ＩＣカード等の取扱い

(ｱ) 職員等は、自己の管理するＩＣカード等に関し、次の事項を遵守しな

ければならない。

ａ　職員等は、個人又は複数の者に対して貸与されたＩＣカード等を他の者に貸与してはならない。

ｂ　業務上必要のないときは、ＩＣカード等をカードリーダ又はパソコン等の端末のスロット等から抜いておかなければならない。

ｃ　ＩＣカード等を紛失した場合には、速やかに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告し、指示に従わなければならない。

(ｲ) 情報セキュリティ管理者は、ＩＣカード等の紛失等の報告があった場合は、当該ＩＣカード等を使用したアクセス等を速やかに停止しなければならない。

(ｳ) 情報セキュリティ管理者は、ＩＣカード等を切り替える場合は、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

イ　ＩＤの取扱い

職員等は、自己の管理するＩＤに関し、次の事項を遵守しなければならない。

(ｱ) 自己が利用しているＩＤは、他の者に利用させてはならない。

(ｲ) 共用ＩＤを利用する場合は、当該共用ＩＤの利用者以外に利用させてはならない。

ウ　パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次に掲げる事項を遵守しなければならない。

(ｱ) パスワードは、他の者に知られないように管理しなければならない。

(ｲ) パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

(ｳ) パスワードについて、文字数は十分な長さとし、文字列は想像しにくいものにしなければならない。

(ｴ) パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

(ｵ) 複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

(ｶ) 仮のパスワード（初期パスワード含む。）は、最初にログインした時点に変更しなければならない。

(ｷ) サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。

(ｸ) 職員等間でパスワードを共有してはならない（ただし、共用 ID に対するパスワードは除く。）。

7　技術的セキュリティ

(1) コンピュータ及びネットワークの管理

ア　フォルダ及びファイルの共有等

(ｱ) 課室等内のフォルダ及びファイル共有については、所属職員等が適正に管理しなければならない。

(ｲ) 情報セキュリティ管理者は、フォルダ及びファイルを共有させる場合は、原則として課室等の単位で構成し、職員等が他の課室等のフォルダ及びファイルを閲覧及び使用できないようにしなければならない。ただし、統括情報セキュリティ責任者が認めたときは、この限りでない。

(ｳ) 情報セキュリティ管理者は、住民の個人情報、人事記録等の特定の職員等しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一課室等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

イ　バックアップの実施

情報セキュリティ管理者は、ファイルサーバ等に記録された情報についてサーバの冗長化対策にかかわらず、必要に応じて定期的にバックアップを実施するものとする。

ウ　他の団体との情報システムに関する情報等の交換

情報セキュリティ管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合は、その取扱いに関する事項をあらかじめ定め、統括情報セキュリティ責任者及び情報セキュリティ責任者の許可を得なければならない。

エ　システム管理記録及び作業の確認

(ｱ) 情報セキュリティ管理者は、所管する情報システムの運用において実施した作業内容について記録を作成しなければならない。

(ｲ) 情報セキュリティ管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理しなければならない。

(ｳ) 統括情報セキュリティ責任者、情報セキュリティ管理者又は情報セキュリティ担当者及び契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、必ず２名以上で作業し、互いにその作業を確認しなければならない。

オ　情報システム仕様書等の管理

情報セキュリティ管理者は、所管する情報システムのネットワーク構成図及び情報システム仕様書について、記録媒体の種類にかかわらず、業務上必要とする者以外の者が閲覧し、又は紛失等しないように適正に管理しなければならない。

カ　ログの取得等

(ｱ) 情報セキュリティ管理者は、所管する情報システムの各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

(ｲ) 情報セキュリティ管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。

(ｳ) 情報セキュリティ管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について、点検又は分析を実施しなければならない。

キ　障害記録

情報セキュリティ管理者は、所管する情報システムにおいて、職員等からのシステム障害の報告内容、システム障害に対する処理結果及び原因等を記録し、適正に保存しなければならない。

ク　ネットワークの接続制御、経路制御等

(ｱ) 統括情報セキュリティ責任者は、フィルタリング及びルーティングについて設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

(ｲ) 統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

ケ　外部の者が利用できるシステムの分離等

情報セキュリティ管理者は、所管する情報システムで外部の者が利用できるシステムについて、必要に応じて他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

コ　外部ネットワークとの接続制限等

(ｱ) 情報セキュリティ管理者は、所管するネットワークを外部ネットワークと接続しようとする場合は、CISO 及び統括情報セキュリティ責任者の許可を得なければならない。

(ｲ) 情報セキュリティ管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

(ｳ) 情報セキュリティ管理者は、接続した外部ネットワークの瑕疵（かし）によりデータの漏えい、破壊、改ざん、システムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

(ｴ) 情報セキュリティ管理者は、ウェブサーバ等をインターネットに公開する場合は、庁内ネットワークへの侵入を防御するため、ファイアウォ

ール等を外部ネットワークとの境界に設置した上で接続しなければならない。

(ｵ) 情報セキュリティ管理者は、接続した外部ネットワークのセキュリティに問題が認められ､情報資産に脅威が生じることが想定される場合は、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

サ　複合機のセキュリティ管理

(ｱ) 統括情報セキュリティ責任者は、複合機を調達する場合は、当該複合機の機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じて適正なセキュリティ要件を策定しなければならない。

(ｲ) 統括情報セキュリティ責任者は、複合機の機能について適正な設定等を行うことにより、運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

(ｳ) 統括情報セキュリティ責任者は、複合機の運用を終了する場合は、複合機の持つ電磁的記録媒体の全ての情報を抹消する又は再利用できないようにする対策を講じなければならない。

シ　IoT 機器を含む特定用途機器のセキュリティ管理

統括情報セキュリティ責任者は､特定用途機器について､取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

ス　無線ＬＡＮ及びネットワークの盗聴対策

(ｱ) 統括情報セキュリティ責任者は、無線ＬＡＮの利用を認める場合は、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

(ｲ) 統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

セ　電子メールのセキュリティ管理

(ｱ) 統括情報セキュリティ責任者は、権限のない者が外部から外部への電子メールの転送ができないように電子メールサーバを設定しなければならない。

(ｲ) 統括情報セキュリティ責任者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

(ｳ) 統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信ができないようにしなければならない。

(ｴ) 統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知し

なければならない。

(ｵ) 統括情報セキュリティ責任者は、システムの開発、運用、保守等のため庁舎内に常駐している委託事業者の作業員による電子メールアドレス利用について、市と委託事業者との間で利用方法を取り決めなければならない。

(ｶ) 統括情報セキュリティ責任者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことがないよう、添付ファイルの監視等の措置をしなければならない。

ソ　電子メールの利用制限

(ｱ) 職員等は、自動転送機能を用いて電子メールを転送してはならない。

(ｲ) 職員等は、業務上必要のない送信先に電子メールを送信してはならない。

(ｳ) 職員等は、複数人に電子メールを送信する場合は、必要がある場合を除き、電子メールの受信者が他の受信者の電子メールアドレスが分からないようにしなければならない。

(ｴ) 職員等は、重要な電子メールを誤送信した場合は、速やかに情報セキュリティ管理者に報告しなければならない。

(ｵ) 職員等は、職務においてウェブで利用できる電子メール、ネットワークストレージサービス等を使用してはならない。業務上必要な場合は、情報セキュリティ管理者の許可を得なければならない。

タ　電子署名及び暗号化

(ｱ) 職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、電子署名、パスワード等による暗号化等のセキュリティを考慮して、送信しなければならない。

(ｲ) 職員等は、暗号化を行う場合は、CISOが定める以外の方法を用いてはならない。また、CISOが定めた方法で暗号のための鍵を管理しなければならない。

(ｳ) CISOは、電子署名の正当性を検証するための情報又は手段を署名検証者へ安全に提供しなければならない。

チ　無許可ソフトウェアの導入等の禁止

(ｱ) 職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。ただし、業務上必要があると認める場合は、情報セキュリティ管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者は、当該ソフトウェアのライセンスを管理しなければならない。

(ｲ) 職員等は、不正にコピーしたソフトウェアを利用してはならない。

ツ　機器構成の変更の制限

職員等は、パソコン及びモバイル端末に対し機器の改造、増設及び交換を行ってはならない。ただし、業務上必要があると認める場合は、情報セキュリティ管理者の許可を得て、パソコン及びモバイル端末に対し機器の改造、増設及び交換を行うことができる。

テ　業務外ネットワークへの接続の禁止

(ｱ) 職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう統括情報セキュリティ責任者によって定められたネットワークと異なるネットワークに接続してはならない。

(ｲ) 統括情報セキュリティ責任者は、支給した端末について、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。

ト　業務以外の目的でのウェブ閲覧の禁止

(ｱ) 職員等は、市の情報システムにおいて、業務以外の目的でウェブを閲覧してはならない。

(ｲ) 統括情報セキュリティ責任者は、市の情報システムにおいて、職員等がウェブを利用する場合に、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

ナ　Web 会議サービスの利用時の対策

(ｱ) 統括情報セキュリティ責任者は、Web 会議を適切に利用するための利用手順を定めなければならない。

(ｲ) 職員等は、市の定める利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

(ｳ) 職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

(ｴ) 職員等は、外部から Web 会議に招待される場合は、情報セキュリティ管理者の許可を得たうえで、必要に応じて利用申請を行い、承認を得なければならない。

ニ　ソーシャルメディアサービスの利用

(ｱ) 情報セキュリティ管理者は、市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

ａ　市のアカウントによる情報発信が、実際の市のものであることを明らかにするために、市の自己管理 Web サイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

ｂ　パスワードや認証のためのコード等の認証情報及びこれを記録した

媒体（ハードディスク、USB メモリ、紙等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

(ｲ) 機密性２以上の情報はソーシャルメディアサービスで発信してはならない。

(ｳ) ソーシャルメディアサービスごとの責任者を定めなければならない。

(ｴ) アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

(ｵ) 可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、市の自己管理 Web サイトに当該情報を掲載して参照可能とすること。

(2) アクセス制御等

ア　アクセス制御等

(ｱ) アクセス制御

統括情報セキュリティ責任者又は情報セキュリティ管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないようにシステム上の制限をしなければならない。

(ｲ) 利用者ＩＤ等の取扱い

a　情報セキュリティ管理者は、所管する情報システムに係る利用者の登録、変更、抹消等の情報管理並びに職員等の異動、出向及び退職者に伴う利用者ＩＤ等の取扱いを定めなければならない。

b　職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、当該情報システムを所管する情報セキュリティ管理者に報告しなければならない。

c　情報セキュリティ管理者は、所管する情報システムについて、利用されていないＩＤ等が放置されないよう、人事管理部門と連携し、点検しなければならない。

(ｳ) 特権を付与されたＩＤの管理等

a　情報システムを所管する情報セキュリティ管理者は、管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理しなければならない。

b　情報システムを所管する情報セキュリティ管理者の特権を代行する者は、当該システムを所管する情報セキュリティ管理者が指名した者でなければならない。

c　情報システムを所管する情報セキュリティ管理者は、管理者権限等の特権を付与されたＩＤ及びパスワードの変更について、委託事業者に行わせてはならない。

d　情報システムを所管する情報セキュリティ管理者は、管理者権限等の特権を付与されたＩＤ及びパスワードについて、職員等の端末等の

パスワードよりも定期変更、入力回数制限などのセキュリティ機能を強化しなければならない。

ｅ　情報システムを所管する情報セキュリティ管理者は、特権を付与されたＩＤを初期設定以外のものに変更しなければならない。

イ　職員等による外部からのアクセス等の制限

(ｱ) 職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者及び当該情報システムを管理する情報セキュリティ管理者の許可を得なければならない。

(ｲ) 統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを許可する場合は、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

(ｳ) 統括情報セキュリティ責任者は、外部からのアクセスを許可する場合は､システム上利用者の本人確認を行う機能を確保しなければならない。

(ｴ) 統括情報セキュリティ責任者は、外部からのアクセスを許可する場合は、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

(ｵ) 統括情報セキュリティ責任者及び情報セキュリティ管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合は、セキュリティ確保のために必要な措置を講じなければならない。

(ｶ) 職員等は、外部から持ち込み、又は持ち帰ったパソコン等の端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、情報セキュリティ管理者の許可を得るか、もしくは情報セキュリティ管理者によって事前に定義されたポリシーに従って接続しなければならない。

(ｷ) 統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを原則として禁止しなければならない。ただし、統括情報セキュリティ責任者が接続することについてやむを得ないと認める場合は、利用者のＩＤ、パスワード及び生体認証に係る情報等の認証情報並びにこれを記録した媒体（ＩＣカード等）による認証に加えて通信内容の暗号化などを行った上で、接続することができる。

ウ　自動識別の設定

統括情報セキュリティ責任者及び情報セキュリティ管理者は、庁内のネットワークで使用される機器について、機器固有情報によってパソコン、モバイル端末等の端末とネットワークとの接続の可否が自動的に識別されるように設定しなければならない。

エ　ログイン時の表示等

情報セキュリティ管理者は、所管する情報システムについて、ログイン

時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるように設定しなければならない。

オ　認証情報の管理

(ｱ) 情報システムを所管する情報セキュリティ管理者は、職員等の認証情報を厳重に管理しなければならない。この場合において、認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

(ｲ) 情報システムを所管する情報セキュリティ管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。

(ｳ) 情報システムを所管する情報セキュリティ管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

カ　特権による接続時間の制限

情報システムを所管する情報セキュリティ管理者は、管理者権限等の特権を付与された場合は、庁内ネットワーク及び情報システムへの接続時間を必要最小限にしなければならない。

(3) システム開発、導入、保守等

ア　情報システムの調達

(ｱ) 統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、情報システムの開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

(ｲ) 統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

イ　情報システムの開発

(ｱ) システム開発における責任者及び作業者の特定

情報システムを所管する情報セキュリティ管理者は、システム開発の責任者及び作業者を特定し、及びシステム開発のための規則を作成しなければならない。

(ｲ) システム開発における責任者及び作業者のＩＤの管理

a　情報システムを所管する情報セキュリティ管理者は、システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後は、開発用ＩＤを削除しなければならない。

b　情報システムを所管する情報セキュリティ管理者は、システム開発

の責任者及び作業者のアクセス権限を設定しなければならならない。

(ｳ) システム開発に用いるハードウェア及びソフトウェアの管理

a　情報システムを所管する情報セキュリティ管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

b　情報システムを所管する情報セキュリティ管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合は、当該ソフトウェアをシステムから削除しなければならない。

ウ　情報システムの導入

(ｱ) 開発環境及び運用環境の分離並びに移行手順の明確化

a　情報システムを所管する情報セキュリティ管理者は、システム導入の際は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

b　情報システムを所管する情報セキュリティ管理者は､システム開発、保守及びテスト環境からシステム運用環境への移行について、システム開発及び保守計画の策定時に手順を明確にしなければならない。

c　情報システムを所管する情報セキュリティ管理者は､システム開発、保守及びテスト環境からシステム運用環境への移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

d　情報システムを所管する情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

(ｲ) テスト

a　情報システムを所管する情報セキュリティ管理者は､新たに情報システムを導入する場合は、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

b　情報システムを所管する情報セキュリティ管理者は、運用テストを行う場合は、あらかじめ擬似環境による操作確認を行わなければならない。

c　情報システムを所管する情報セキュリティ管理者は、個人情報及び機密性の高いデータを、テストデータに使用してはならない。

d　情報システムを所管する情報システム管理者は、開発したシステムについて受け入れテストを行う場合は、開発した組織及び導入する組織が、それぞれ独立したテストを行わなければならない。

エ　システムの開発及び保守に関連する資料等の整備並びに保管

(ｱ) 情報システムを所管する情報セキュリティ管理者は、システムの開発及び保守に関連する資料並びにシステム関連文書を適正に整備及び保管

しなければならない。

(ｲ) 情報システムを所管する情報セキュリティ管理者は、テスト結果を一定期間保管しなければならない。

(ｳ) 情報システムを所管する情報セキュリティ管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

オ　情報システムにおける入出力データの正確性の確保

(ｱ) 情報システムを所管する情報セキュリティ管理者は、情報システムに入力されるデータについて、範囲及び妥当性のチェック機能並びに不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

(ｲ) 情報システムを所管する情報セキュリティ管理者は、故意又は過失により情報が改ざんされ、又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

(ｳ) 情報システムを所管する情報セキュリティ管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、及び出力されるように情報システムを設計しなければならない。

カ　情報システムの変更管理

情報システムを所管する情報セキュリティ管理者は、情報システムを変更した場合は､プログラム仕様書等の変更履歴を作成しなければならない。

キ　開発用及び保守用のソフトウェアの更新等

情報システムを所管する情報セキュリティ管理者は、開発及び保守用のソフトウェア等を更新又はパッチの適用をする場合は、他の情報システムとの整合性を確認しなければならない。

ク　システム更新及び統合時の検証等

情報システムを所管する情報セキュリティ管理者は、システム更新及び統合時に伴うリスク管理体制の構築、移行基準の明確化並びに更新及び統合後の業務運営体制の検証を行わなければならない。

(4) 不正プログラム対策

ア　統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正プログラム対策として、次に掲げる措置を講じなければならない。

(ｱ) 外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムの情報システムへの侵入を防止すること。

(ｲ) 外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止すること。

(ｳ) コンピュータウイルス等の不正プログラムの情報を収集し、必要に応じ、職員等に対して注意喚起すること。
(ｴ) 所掌するサーバ及びパソコン等の端末にコンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させること。
(ｵ) 不正プログラム対策ソフトウェアのパターンファイルを常に最新の状態に保つこと。
(ｶ) 不正プログラム対策のソフトウェアを常に最新の状態に保つこと。
(ｷ) 業務で利用するソフトウェアは、パッチ、バージョンアップ等の開発元のサポートが終了したソフトウェアを利用しないこと。また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認すること。

イ　情報セキュリティ管理者の措置事項

情報システムを所管する情報セキュリティ管理者は、不正プログラム対策に関し、次に掲げる措置を講じなければならない。
(ｱ) 所管する情報システムにコンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させること。
(ｲ) 不正プログラム対策ソフトウェアのパターンファイルを常に最新の状態に保つこと。
(ｳ) 不正プログラム対策のソフトウェアを常に最新の状態に保つこと。
(ｴ) インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合は、コンピュータウイルス等の感染を防止するために市が管理している媒体以外を職員等に利用させないこと。また、不正プログラムの感染及び侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施すること。
(ｵ) 不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報システム管理者が許可した職員を除く職員等に当該権限を付与しないこと。

ウ　職員等の遵守事項

職員等は、不正プログラム対策に関し、次に掲げる事項を遵守しなければならない。
(ｱ) パソコン及びモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は､当該ソフトウェアの設定を変更しないこと。
(ｲ) 外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行うこと。
(ｳ) 差出人が不明又は不自然にファイルが添付された電子メールを受信した場合は、速やかに削除すること。
(ｴ) 端末に対して、不正プログラム対策ソフトウェアによるフルチェック

を定期的に実施すること。ただし、リアルタイムチェックと共存できない場合は、その限りでない。

(ｵ) 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行うこと。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルをLGWAN接続系に取り込む場合は無害化を行うこと。

(ｶ) 統括情報セキュリティ責任者が提供するウイルス情報を常に確認すること。

(ｷ) コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行うこと。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末においてLANケーブルの取り外しや、通信を行わない設定への変更などを実施すること。

エ　専門家の支援体制

統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

(5) 不正アクセス対策

ア　統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正アクセス対策として、次に掲げる措置を講じなければならない。

(ｱ) 使用されていないポートを閉鎖すること。

(ｲ) 重要な情報システムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査すること。

(ｳ) 不要なサービスについて、機能を削除又は停止すること。

(ｴ) 不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ責任者及び情報システム管理者へ通報するよう、設定すること。

(ｵ) 統括情報セキュリティ責任者は、PoCと連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築すること。

イ　攻撃への対処

CISO及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、総務省、埼玉県等と連絡を密にして情報の収集に努めなければならない。

ウ　記録の保存

CISO及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）に違反する等犯罪の可能性がある場合は、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

エ　内部からの攻撃

統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、職員等及び委託事業者が使用しているパソコン等の端末からのサーバ等に対する攻撃及び外部のサイトに対する攻撃を監視しなければならない。

オ　職員等による不正アクセス

統括情報セキュリティ責任者及び情報セキュリティ管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

カ　サービス不能攻撃

統括情報セキュリティ責任者及び情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

キ　標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

(6) セキュリティ情報の収集

ア　セキュリティホールに関する情報収集及び共有、ソフトウェアの更新等

統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

イ　不正プログラム等のセキュリティ情報の収集及び周知

統括情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ、対応方法について職員等に周知しなければならない。

ウ　情報セキュリティに関する情報の収集及び共有

統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関

係者間で共有しなければならない。また、情報セキュリティに関する社会環境、技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

8　運用

(1) 情報システムの監視

ア　統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

イ　統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

ウ　統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、外部と常時接続するシステムを常時監視しなければならない。

エ　暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入しなければならない。

(2) 情報セキュリティポリシーの遵守状況の確認

ア　遵守状況の確認及び対処

(ｱ) 情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題があると認めた場合は、速やかに CISO 及び統括情報セキュリティ責任者に報告しなければならない。

(ｲ) CISO は、発生した情報セキュリティポリシーに関する問題について、適正かつ速やかに対処しなければならない。

(ｳ) 統括情報セキュリティ責任者及び情報システムを所管する情報セキュリティ管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には、適正かつ速やかに対処しなければならない。

イ　パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

CISO 及び CISO が指名した者は、不正アクセス、不正プログラム等の調査のために職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体のログ、電子メールの送受信記録等の利用状況を調査することができる。

ウ　職員等の報告義務

(ｱ) 職員等は、情報セキュリティポリシーに対する違反行為を発見した場

合は、直ちに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告を行わなければならない。

(ｲ) 統括情報セキュリティ責任者は、当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると判断した場合において、職員等は、次号アに規定する計画に従って適正に対処しなければならない。

(3) 侵害時の対応等

ア　緊急時対応計画の策定

CISOは、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生し、又は発生するおそれがある場合の連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するための計画（以下「緊急時対応計画」という。）をあらかじめ定めておかなければならない。

イ　緊急時対応計画に盛り込むべき内容

緊急時対応計画の内容は、次のとおりとする。

(ｱ) 関係者の連絡先に関すること。

(ｲ) 発生した事案に係る報告すべき事項に関すること。

(ｳ) 発生した事案への対応措置に関すること。

(ｴ) 再発防止措置の策定に関すること。

ウ　業務継続計画との整合性の確保

CISOは、自然災害、大規模及び広範囲にわたる疾病等に備えて別途業務継続計画を策定し、当該計画と情報セキュリティポリシーとの整合性を確保しなければならない。

エ　緊急時対応計画の見直し

CISOは、情報セキュリティを取り巻く状況の変化、組織体制の変動等に対応するため、必要に応じて緊急時対応計画の内容を見直さなければならない。

(4) 例外措置

ア　例外措置の許可

情報セキュリティ管理者は、情報セキュリティ関係の規程を遵守することが困難な状況であり、かつ、行政事務の適正な遂行を継続するため遵守事項と異なる方法を採用する又は遵守事項を実施しないことについて合理的な理由がある場合は、あらかじめCISOの許可を得た上で、例外措置を取ることができる。

イ　緊急時の例外措置

情報セキュリティ管理者は、行政事務の遂行に緊急を要するなどの場合であって、例外措置を実施することが不可避のときは、事後速やかにCISOに報告しなければならない。

ウ　例外措置の申請書の管理

CISO は、例外措置の申請書及び審査結果を適正に保管し、及び定期的に申請状況を確認しなければならない。

(5) 法令遵守

職員等は、職務の遂行において使用する情報資産を保護するために、次に掲げる法律及び条例のほか関係法令等を遵守し、これに従わなければならない。

ア　地方公務員法（昭和２５年法律第２６１号）

イ　著作権法（昭和４５年法律第４８号）

ウ　不正アクセス行為の禁止等に関する法律

エ　個人情報の保護に関する法律（平成１５年法律第５７号）

オ　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７号）

カ　サイバーセキュリティ基本法（平成２６年法律第１０４号）

キ　ふじみ野市個人番号の利用事務等に関する条例（平成２７年ふじみ野市条例第４５号）

(6) 懲戒処分等

ア　懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法に定める懲戒処分の対象とする。

イ　違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合は、速やかに次に掲げる措置を講じなければならない。

(ｱ) 統括情報セキュリティ責任者は、違反を確認した場合は、当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めること。

(ｲ) 情報システムを所管する情報セキュリティ管理者等は、違反を確認した場合は、速やかに統括情報セキュリティ責任者及び当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めること。

(ｳ) 統括情報セキュリティ責任者は、(ｱ)又は(ｲ)に規定する措置の求めをした後もなお改善されない場合は、当該職員等のネットワーク又は情報システムを使用する権利を停止又は剥奪することができる。この場合において、統括情報セキュリティ責任者は、職員等の権利を停止又は剥奪した旨を CISO 及び当該職員等が所属する課室等の情報セキュリティ管理者に速やかに通知しなければならない。

9　業務委託と外部サービスの利用

(1) 業務委託

ア　委託事業者の選定基準

(ｱ) 情報セキュリティ管理者は、委託事業者の選定に当たり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

(ｲ) 情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定しなければならない。

イ　契約項目

情報セキュリティ管理者は、情報システムの運用、保守等を業務委託する場合は、委託事業者との間で必要に応じて次に掲げる情報セキュリティに関する内容が含まれる契約を締結しなければならない。

(ｱ) 情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

(ｲ) 委託事業者の責任者、委託内容、作業者及び作業場所の特定

(ｳ) 提供されるサービスレベルの保証

(ｴ) 委託事業者にアクセスを許可する情報の種類及び範囲並びにそのアクセス方法の明確化など、情報のライフサイクル全般での管理の実施

(ｵ) 委託事業者の従業員に対する教育の実施

(ｶ) 提供された情報の目的外利用及び委託事業者以外の者への提供の禁止

(ｷ) 業務上知り得た情報の守秘義務

(ｸ) 再委託に関する制限事項の遵守

(ｹ) 委託業務終了時の情報資産の返還、廃棄等

(ｺ) 委託業務の定期報告及び緊急時の報告義務

(ｻ) 市による監査及び検査

(ｼ) 市による情報セキュリティインシデント発生時の公表

(ｽ) 情報セキュリティポリシーが遵守されなかった場合の損害賠償その他委託事業者の違反に関する内容

ウ　確認及び措置等

情報セキュリティ管理者は、委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、その内容について契約を締結しなければならない。この場合において、その内容を必要に応じて統括情報セキュリティ責任者に報告するとともに、その重要度に応じてCISOに報告しなければならない。

(2) 外部サービスの利用（機密性２以上の情報を取り扱う場合）

ア　外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は､次に掲げる事項を含む外部サービス(機密性２以上の情報を取り扱う場合）の利用に関する規定を整備すること。

(ｱ) 外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下「外部サービス利用判断基準」という。）
(ｲ) 外部サービス提供者の選定基準
(ｳ) 外部サービスの利用申請の許可権限者と利用手続
(ｴ) 外部サービス管理者の指名と外部サービスの利用状況の管理

イ　外部サービスの選定

(ｱ) 情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。
(ｲ) 情報セキュリティ責任者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。
ａ　外部サービスの利用を通じて市が取り扱う情報の外部サービス提供者における目的外利用の禁止
ｂ　外部サービスの提供者における情報セキュリティ対策の実施内容及び管理体制
ｃ　外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、市の意図しない変更が加えられないための管理体制
ｄ　外部サービス提供者の資本関係・役員等の情報、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定
ｅ　情報セキュリティインシデントへの対処方法
ｆ　情報セキュリティ対策その他の契約の履行状況の確認方法
ｇ　情報セキュリティ対策の履行が不十分な場合の対処方法
(ｳ) 情報セキュリティ責任者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めること。
(ｴ) 情報セキュリティ責任者は、外部サービスの利用を通じて市が取り扱う情報の格付等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含めること。
ａ　情報セキュリティ監査の受入れ
ｂ　サービスレベルの保証
(ｵ) 情報セキュリティ責任者は、外部サービスの利用を通じて市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価し

て外部サービス提供者を選定し、必要に応じて市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めること。

(ｶ) 情報セキュリティ責任者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を市に提供し、市の承認を受けるよう、外部サービス提供者の選定条件に含めること。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。

(ｷ) 情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定すること。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めること。

(ｸ) 情報セキュリティ責任者は、外部サービスの特性を考慮したうえで、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行ったうえで、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めること。

(ｹ) 情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断すること。

ウ　外部サービスの利用に係る調達・契約

(ｱ) 情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めること。

(ｲ) 情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めること。

エ　外部サービスの利用承認

(ｱ) 情報セキュリティ責任者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うこと。

(ｲ) 利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。

(ｳ) 利用申請の許可権限者は､外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名すること。

オ　外部サービスを利用した情報システムの導入・構築時の対策

(ｱ) 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定すること。

a　不正なアクセスを防止するためのアクセス制御

b　取り扱う情報の機密性保護のための暗号化

c　開発時におけるセキュリティ対策

d　設計・設定時の誤りの防止

(ｲ) 外部サービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録すること。

カ　外部サービスを利用した情報システムの運用・保守時の対策

(ｱ) 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定すること。

a　外部サービス利用方針の規定

b　外部サービス利用に必要な教育

c　取り扱う資産の管理

d　不正アクセスを防止するためのアクセス制御

e　取り扱う情報の機密性保護のための暗号化

f　外部サービス内の通信の制御

g　設計・設定時の誤りの防止

h　外部サービスを利用した情報システムの事業継続

(ｲ) 情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備すること。

(ｳ) 外部サービス管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録すること。

キ　外部サービスを利用した情報システムの更改・廃棄時の対策

(ｱ) 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスの利用を終了する際のセキュリティ対策を規定すること。

a　外部サービスの利用終了時における対策

b　外部サービスで取り扱った情報の廃棄

c　外部サービスの利用のために作成したアカウントの廃棄

(ｲ) 外部サービス管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録すること。

(3) 外部サービスの利用（機密性２以上の情報を取り扱わない場合）

ア　外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、以下を含む外部サービス（機密性２以

上の情報を取り扱わない場合）の利用に関する規定を整備すること。
(ｱ) 外部サービスを利用可能な業務の範囲
(ｲ) 外部サービスの利用申請の許可権限者と利用手続
(ｳ) 外部サービス管理者の指名と外部サービスの利用状況の管理
(ｴ) 外部サービスの利用の運用手順

イ　外部サービスの利用における対策の実施
(ｱ) 職員等は、利用するサービスの約款、その他提供条件等から、利用にあたってのリスクが許容できることを確認した上で機密性２以上の情報を取り扱わない場合の外部サービスの利用を申請すること。また、承認時の指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずること。
(ｲ) 情報セキュリティ責任者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。また、承認した外部サービスを記録すること。

10　評価及び見直し

(1) 監査

ア　実施方法

CISOは、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて､その指名した者に監査を行わせることができる。

イ　監査を行う者の要件
(ｱ) 情報セキュリティ監査統括責任者は、監査を実施する場合は、被監査部門から独立した者に対して、監査の実施を依頼する。
(ｲ) 監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者とする。

ウ　監査実施計画の立案及び実施への協力
(ｱ) 情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、ＤＸ推進会議の承認を得るものとする。
(ｲ) 被監査部門は、監査の実施に協力しなければならない。

エ　委託事業者に対する監査

情報セキュリティ監査統括責任者は､委託事業者に情報システムの開発、運用その他情報システムに係る業務を委託している場合は､委託事業者(再委託事業者を含む）に対して、情報セキュリティポリシーの遵守について監査を定期的又は必要に応じて行うものとする。

オ　報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、ＤＸ推進会議に報告しなければならない。

カ　保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した証拠及び報告のための監査調書を紛失等が発生しないように適正に保管しなければならない。

キ　監査結果への対応

(ｱ) CISOは、オの監査結果を踏まえ、指摘事項があった場合は、当該指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。

(ｲ) CISOは、(ｱ)の指摘事項のなかった情報セキュリティ管理者に対しても､指摘事項について同種の課題及び問題点がある可能性が高い場合は、当該課題及び問題点の有無を確認させなければならない。なお、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。

ク　情報セキュリティポリシー及び関係規程等の見直し等への活用

CISOは､監査結果を情報セキュリティポリシー及び関係規程等の見直しその他情報セキュリティ対策の見直し時に活用しなければならない。

(2) 自己点検

ア　実施方法

(ｱ) 統括情報セキュリティ責任者は､情報セキュリティ管理者と連携して、所管するネットワーク及び情報システムに係る情報セキュリティ対策状況について、定期的又は必要に応じて自己点検を実施しなければならない。

(ｲ) 統括情報セキュリティ責任者は､情報セキュリティ管理者と連携して、情報セキュリティポリシーに沿った情報セキュリティ対策状況について、定期的又は必要に応じて自己点検を行わなければならない。

イ　報告

統括情報セキュリティ責任者は、自己点検の結果及び当該結果による改善策を取りまとめ、ＤＸ推進会議に報告しなければならない。

ウ　自己点検結果の活用

(ｱ) 職員等は、自己点検の結果により、自己の権限の範囲内で改善を図らなければならない。

(ｲ) CISOは、この点検結果を情報セキュリティポリシー及び関係規程等の見直しその他情報セキュリティ対策の見直し時に活用しなければならない。

(3) 情報セキュリティポリシー及び関係規程等の見直し

CISOは、情報セキュリティ監査、自己点検の結果、情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について定期的及び重大な変化が発生した場合は随時に評価を行うものとし、及

び必要があると認めた場合は、ＤＸ推進会議に諮った上で、情報セキュリティポリシー及び関係規程等の見直しを行うものとする。